

## МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» РТУ МИРЭА

### РТУ МИРЭА

Институт кибербезопасности и цифровых технологий Кафедра КБ-2 «Прикладные информационные технологии»

Практическая работа № 7 по дисциплине «Безопасность Операционных систем» «Безопасность в Linux»

Задание на практику:

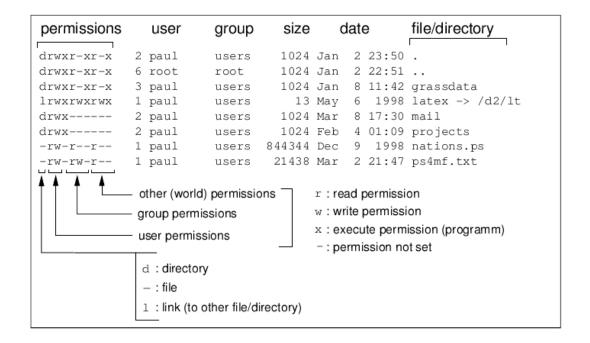
Управление локальными пользователями и группами Linux

- 1. Создайте пользователя user, сделав его участником группы wheel
- 2. Убедитесь, что пользователь был создан и задайте пароль для него
  - \$ tail -2 /etc/passwd
  - \$ passwd user
- 3. Войдите в учетную запись user и изучите сведения о пользователе, группе и отобразите текущий каталог.
- 4. Просмотрите переменные, которые указывают на домашний каталог и пути, где происходит поиск исполняемых файлов
  - 5. Войдите в учетную запись root, используя команду su
  - 6. Повторите действия 3, 4
  - 7. Войдите в учетную запись root, используя команду su -
  - 8. Повторите действия 3, 4
  - 9. Проанализируйте разницу
  - 10. Изучите последние строки в /var/log/messages
  - 11. Выполните команды от пользователя user
  - \$ echo "nameserver 1.1.1.1" | tee -a /etc/resolv.conf /dev/null
  - \$ echo "nameserver 1.1.1.1" | sudo tee -a /etc/resolv.conf /dev/null

- \$ vi /etc/motd
- \$ sudo vi /etc/motd

# 12. Проанализируйте разницу

## Разрешения файловой системы



#### **Linux File Permission Codes**

Permissions	Binary	Octal	Description	
	000	0	No permissions	
X	001	1	Execute-only permission	
- W -	010	2	Write-only permission	
-WX	011	3	Write and execute permissions	
r	100	4	Read-only permission	
r-x	101	5	Read and execute permissions	
rw-	110	6	Read and write permissions	
rwx	111	7	Read, write, and execute permissions	

Разрешения по умолчанию

umask Value Octal (xyz)	Default File Permissions	666 - xyz	Default Directory Permissions	777 - xyz
000	rw-rw-rw	666	rwxrwxrwx	777
002	rw-rw-r	664	rwxrwxr-x	775
022	rw-rr	644	rwxr-xr-x	755
026	rw-r	640	rwxr-xx	751
046	rww	620	rwx-wxx	731
062	rwr	604	rwxxr-x	715
066	rw	600	rwxxx	711
222	rrr	444	r-xr-xr-x	555
600	rw-rw-	066	xrwxrwx	177
666		000	XX	111
777		000		000

- 13. Отобразите значение по умолчанию для пользователя user
- \$ umask
- 14. Создайте директрию и файл, чтобы увидеть как пользовательская маска влияет на разрешения.
  - \$ mkdir /tmp/catalog
  - \$ ls -ld /tmp/catalog
  - \$ touch /tmp/catalog/file
  - \$ ls -l /tmp/catalog/file
- 15. Измените маску user таким образом, чтобы новые файлы создавались с доступом только на чтение для группы и без прав доступа для других пользователей.
  - \$ umask 027
  - \$ touch /tmp/catalog/file\_1
  - \$ ls -1 /tmp/catalog/file 1

16. Измените маску по умолчанию для пользователя user, чтобы запретить весь доступ для пользователей, не относящихся к группе.

• \$ echo "umask 007" » ~/.bashrc

• \$ cat ~/.bashrc

17. Войдите еще раз от имени пользователя user, и проверьте сохранилась ли измененная маска.

• \$ umask

**ACL** 

18. Создайте файл /directory/file и группу workers. Добавьте пользователя user в группу workers. Измените группу владельцев directory на workers.

• # groupadd workers

• # usermod -G workers user

• # mkdir /directory

• # echo "Hello from file" > /directory/file

•# chown -R :workers /directory

19. Войдите в систему под пользователем user.

Например:

\$ su - user

Прочтите файл:

\$ cat /directory/file

20. Установите ACL для пользователя user, таким образом, чтобы он не имел доступа ни к существующим файлам, ни к созданным в будущем в каталоге /directory.

# setafacl -Rm u:user:- /directory

# setfacl -m d:u:user:- /directory

- 21. Попробуйте прочесть файл /directory/file и создать новый
- 22. Просмотрите и проанализируйте ACL для /directory

# getfacl /directroy